HASIL CEK_1808048032

by Abdul Hadi 1808048032

Submission date: 06-Jul-2019 08:09AM (UTC+0700)
Submission ID: 1149529274
File name: CEK_1808048032.pdf (611.09K)
Word count: 2760
Character count: 17473

FORENSIK BUKTI DIGITAL PADA SOLID STATE DRIVE (SSD) NVMe MENGGUNAKAN METODE NATIONAL INSTITUTE STANDARDS and TECHNOLOGY (NIST)

Abstrak. *Bukti digital sangat penting untuk membuktikan kasus penyidikan kejahatan komputer yang melibatkan perangkat media penyimpanan. Perkembangan teknologi media penyimpanan saat ini dituntut cepat dalam membaca dan menulis data menyesuaikan perkembangan perangkat keras lainnya seperti processor dan Random Access Memory (RAM). Teknologi media penyimpanan yang baru saat ini adalah Solid State Drive Non-volatile Memory Express (SSD NVMe) yang berbeda dengan pendahulunya yaitu SSD SATA dari segi kecepatan dan bentuk interfacenya. Secara default sistem operasi Windows 10 sudah terapasang fasilitas TRIM dengan mode enable, fasilitias ini secara otomatis akan menghapus data lama pada sebuah sektor sebelum ditempatkan data baru, sehingga SSD NVMe akan membaca data secara optimal. Akan tetapi dengan adanya fungsi TRIM pada SSD NVMe memiliki efek negatif pada analisis forensik khususnya pada recovery data. Tujuan penelitian melakukan perbandingan dan kemampuan tools forensics untuk mengembalikan bukti digital pada SSD NVMe pada sistem operasi Windows 10 dengan file sistem NTFS. Penelitian ini menggunakan metode National Institute Standards and Technology (NIST) dengan tahapan Collection, Examination, Analysis dan Reporting. Skenario yang digunakan adalah static forensics, tool yang digunakan untuk akuisisi FTK Imager dan tools analisis Autopsy dan RecoverMyFile. Output yang diharapkan berupa alur proses analisis untuk mendapatkan barang bukti digital yang terhapus dan membandingkan tools yang paling efektif dalam melakukan analisis bukti digital pada SSD NVMe.*

Kata kunci: *SSD NVMe, bukti digital, NIST, komputer forensik*

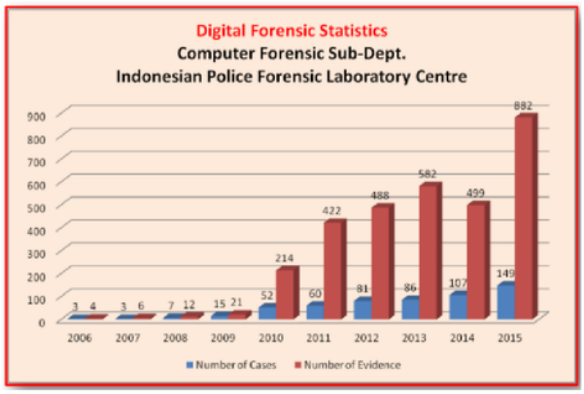
Abstract. *Digital evidence is very important for verifying computer crime investigation involving the storage of the computer. The evolution technology of storage computer must be improved for reading and writing speed data because storage must be adapted for evolution hardware of computer like the processor and Random Access Memory (RAM). The latest Storage technology is Solid State Drive Non-Volatile Memory Express (SSD NVMe) it more different from SSD SATA by comparison speed and interface. For optimizing the speed of SSD NVME operating system Windows 10 with default installed TRIM enable mode, TRIM can automatically delete old files at a sector before creating a new file. But with TRIM facility with enable mode can be taken negative effect for analysis digital forensics especially at data recovery. The purpose of this research is making comparison and capability of tools forensics for recovery digital evidence at the Windows 10 operating system with NTFS file system. This research used National Institute Standards and Technology (NIST) method with four stages are Collection, Examination, Analysis, and Reporting. The scenario this research used static forensics, acquisition using FTK Imager tool and for analyzing digital evidence using autopsy and recoverMyFile tools. The expectation in this research are finding deleted digital evidence and comparison with other tools for the most effective tools analysis digital evidence.*

Keywords*: SSD NVMe, digital forensics, NIST, computer forensics*

1. PENDAHULUAN

Kejahatan komputer merupakan kejahatan yang melibatkan teknologi, seiring perkembangan teknologi modus kejahatan komputer atau *cyber computer* juga mengikuti perkembangan teknologi yang ada saat ini (Al-Azhar, 2012). Jika diamati beberapa kasus kejahatan komputer model dan modus mengalami perubahan maka terbitlah Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektornik (ITE) salah satu tujuannya adalah memberikan rasa aman, keadilan dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi. Disamping itu penanganan tindak kejahatan komputer saat ini masih minim, dari pengambilan barang bukti yang tidak cukup, kesalahan akuisisi pengambilan barang bukti, atau bahkan sampai hilang atau rusaknya barang bukti.

Model-model kejahatan terkait dengan komputer dikuatkan dengan berita dan fakta di media massa, diantaranya penyitaan barang bukti perangkat komputer dan media penyimpanan komputer sebagaimana diberitakan oleh oleh detik.com Selasa, 20 Februari 2018 dengan judul "Geledah Ruang Kerja Bupati Imas, KPK Sita Dokumen dan Komputer" berita yang dikabarkan media massa tersebut kasus suap terhadap Bupati Subang secara bersama-sama terkait pengurusan perizinan, penyidik menggeledah tiga lokasi dan menyita sejumlah dokumen dan barang bukti elektronik. Di Indonesia terjadi kenaikan kasus kejahatan komputer setiap tahunnya. Dalam 10 tahun terakhir terdapat 563 kasus kejahatan dengan total jumlah barang bukti elektronik sebanyak 3.130 unit. Statistik tersebut menunjukkan bahwa kejahatan komputer adalah permasalahan serius dalam era digital seperti Gambar 1 (Sumber: Bareskrim puslabfor polri, 2015).



Gambar 1 Statistik *digital forensics* 2006-2015

Adanya kasus-kasus yang diberitakan media massa terkait tindak kejahatan elektronik dan barang bukti elektronik berupa perangkat komputer yang melibatkan media penyimpanan, menjadi pekerjaan yang harus diselesaikan dan dituntaskan oleh penyidik dan penegak hukum guna mengungkap modus, motif dan pelaku tindak kejahatan atau dengan kata lain membuktikan kejahatan terkait dengan barang bukti yang didapatkan. Perkembangan teknologi media penyimpanan saat ini dituntut cepat dalam membaca dan menulis data menyesuaikan perkembangan perangkat keras yang lainnya seperti *processor dan Random Access Memory* (RAM). Teknologi media penyimpanan yang baru saat ini *adalah Solid State Drive Non-volatile Memory Express* (SSD NVMe) yang berbeda dengan SSD SATA pendahulunya dari segi kecepatan dan bentuk interfacenya. Sistem operasi Windows 10 saat ini sudah terpasang secara *default* fasilitas TRIM dengan *mode enable*, fasilitias ini secara otomatis akan menghapus data lama pada sektor sebelum ditempatkan data baru, sehingga SSD NVMe akan membaca data secara optimal. Akan tetapi dengan adanya fungsi TRIM ini pada SSD NVMe memiliki efek negatif pada analisis forensik khususnya pada *recovery* data.

Berdasarkan latar belakang diatas maka perlu dilakukan penelitian dan analisis pada SSD NVMe pada sistem operasi Windows. Penelitian ini akan membahas implementasi forensik digital terhadap barang bukti yaitu SSD NVMe pada file sistem NTFS.

Proses investigasi digital pada penelitian ini menggunakan *static forensics* dengan metode *National Institute Standards and Technology* (NIST), *tool* yang digunakan untuk akuisisi FTK Imager dan *tools* analisis Autopsy dan RecoverMyFile. Output yang diharapkan berupa alur proses analisis untuk mendapatkan barang bukti digital yang terhapus dan membandingkan *tools* yang paling efektif dalam melakukan analisis bukti digital pada SSD NVMe. Penelitian dengan tema sejenis pernah dilakukan beberapa peneliti terdahulu sebagai berikut:

1. Sivashankar, et al (2014) dari *Electronis and telecommunications Reseach Institute*, dengan judul "Design an Implemantation of Non-volatile Memory Express" melakukan uji coba antrian perintah (*command*), *queuing interface*, perbandingan *po* dan latensi pada SSD dan HDD SATA dan SSD NVMe.
2. Imam Mahfudl Nasrulloh (2019) dari Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia, dengan judul "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Menggunakan Metode Statis Forensik". SSD SATA yang terfrozen dijadikan barang bukti digital dengan metode *static forensics*, penelitian menggunakan perangkat lunak forensik Recovery My File, Belkasoft, Forensic Toolkit (FTK) dan Encase. Untuk *tool* akuisisi menggunakan tableau forensic bridge dengan perangkat lunak akuisisi tableau imager. Metode yang digunakan adalah *static forensics* dengan menggunakan *framework* NIST, format file sistem tiap SSD adalah NTFS. Hasil eksaminasi dari SSD yang terfrozen berhasil menemukan artefak dengan *tools* forensik Recovery My File 0,9991 (100%), Autospy 100%, Belkasoft 100%, Forensic Toolkit 92%, Encase 100%. Penelitian ini juga membuat perbandingan antara SSD yang terfrozen dan yang tidak terfrozen dalam pengambilan artefak.
3. Rizdqi Akbar Ramadhan (2017) dari Magister Teknik Informatika, Universitas Islam Indonesia, Yogyakarta, Indonesia, judul "Implementasi dan Analisis Forensika Digital pada Fitur Trim Solid State Drive". Penelitian ini membandingkan tools forensik yang digunakan untuk analisis dan eksaminasi SSD dengan mode TRIM. Hasil penelitian menghasilkan mekanisme TRIM pada SSD saat diaktifkan menimbulkan ndala dalam penyelidikan *digital forensics*. Mekanisme TRIM memiliki pengaruh ketika diaktifkan pada sistem operasi. Sistem operasi yang digunakan adalah windows 7 dengan file sistem NTFS. Metode akuisisi yang digunakan *static forensi* dan *tool* yang digunakan adalah Forensic Toolkit (FTK) dan Sleuth Kit Autopsy.
4. Faiz Albanna (2017) dari Magister Teknik Informatika, Universitas Islam Indonesia, Yogyakarta, Indonesia, dengan judul "Analisis Bukti Digital Pada Frozen Hard Drive Menggunakan Metode Static Forensic". Pada penelitian melakukan analisis *digital forensics* pada HDD yang terinstal aplikasi frozen seperti Deep Freeze, analisis bukti digital dilakukan setelah kondisi komputer dimatikan atau HDD dalam keadaan ter-deep freeze. Hasil dari investigasi pada beberapa file dokumen digital, gambar, *log history* internet dan *log file* terbaru dapat dikembalikan kembali, namun ditemukan tidak pada direktori aslinya atau dengan kata lain terletak pada *unlocated space drive*.
5. Binaya Raj Joshi (2016) dari *School of Interdisciplinary Informatics*, University of Nebraska Omaha, NE, USA, judul "Forensic Analysis of Solid State Drive (SSD)" melakukan perbandingan fitur TRIM pada SSD yang berjalan pada sistem operasi yang berbeda, pada konekoter kabel yang berbeda dan pada file sistem berbeda. Tools yang digunakan untuk mengembalikan artefak adalah Recuva, hasil penelitian menunjukkan hasil yang berbeda saat fitur TRIM diaktifkan dan dinon-aktifkan.

2. LANDASAN TEORI

Digital Forensics

Digital forensics menurut Muhammad Nuh Al-Azhar (2012) merupakan aplikasi bidang ilmu pengatahuan dan teknologi komputer untuk pembuktian hukum (*pro justice*), dalam hal ini adalah untuk membuktikan kejahatan teknologi tinggi atau *computer crime* secara ilmiah (*scientific*), hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut. *Digital forensics* adalah ilmu mengidentifikasi, penggalian, menganalisa, dan meyajikan barang bukti digital yang terdapat pada perangkat penyimpanan elektronik yang digunakan dalam pengadilan hukum, tujuan utama dari analisis forensik adalah untuk mengidentifkasi semua peristiwa, untuk mengatahui efek pada sistem, untuk memperoleh bukti yang diperlukan, untuk mencegah insiden dimasa mendatang dengan mendeteksi teknik berbahaya yang digunakan.

Digital forensics merupakan instrumen untuk menjawab tentang kapan, apa, siapa, dimana, bagaimana, dan mengapa, terkait dengan kejahatan digital (Imam Riadi, Istiyanto & Ashari, 2014). Menurut Wazid, Katal, Goudar & Rao (2013) membagi *digital forensics* pada beberapa kelompok, diantaranya; 1) Komputer Forensik; 2) Memori Forensik; 3) Network Forensik; 4) Mobile Forensik; 5) Database Forensik; 6) Email Forensik. Dan menurut Muhammad Nuh Al-Azhar (2016) pembagian kelompok digital forensik menjadi sepuluh (10) kelompok yaitu: *computer forensics, cyber forensics, triage forensics, malware forensics, memory forensics, anti-forensics, audio forensics, image forensics, video forensics* dan yang terakhir *mobile forensics* seperti Gambar 2.

Gambar 2 Pembagian kelompok keilmuan dibidang *digital forensics*

Solid State Drive Non-volatile Memory Express (SSD NVMe)

Media penyimpanan terdiri dari dua jenis *yaitu non-volatile memory* dan *volatile memory*. Pada *Non-volatile memory* data yang tersimpan tidak akan hilang meskipun aliran listrik terpustus atau komputer dalam keadaan mati contoh media penyimpanan adalah HDD, SSD, USB flashdisk, sedangkan *volatile memory* akan kehilangan data saat aliran listrik terputus contohnya RAM (Silberschatz et al., 2013).

SSD NVMe termasuk media penyimpanan komputer terbaru setelah diluncurkanya SSD SATA. NVMe merupakan teknologi yang dikembangkan untuk mengatasi limitasi dari teknologi yang sudah ada. NVMe memanfaatkan jalur PCIe (slot PCIe, M.2 dan U.2).

Teknologi yang muncul sebelum SSD NVMe adalah M.2 SATA, M.2 SATA menggunakan jalur PCI express 2.0 menggunakan protokol AHCI, sedangkan SSD NVMe memakai 4 jalur PCI express 3.0 secara teoritis 4 GB per detik menggunakan protokol NVMe. Gambar 3 merupakan perbandingan kecepatan baca dan tulis antara media penyimpanan HDD, SSD SATA dan SSD NVMe.

HDD SSD SATA SSD NVMe

Gambar 3 Perbandingan kecepatan baca dan tulis HDD, SSD SATA dan SSD NVME

Kelebihan penggunaan SSD NVMe yang telah diberitakan situs resmi NVM Express adalah sebagai berikut: Peningkatan kinerja, jumlah *command* yang tidak terbatas, manajemen antrian optimal, serial bus lebih cepat dengan multi jalur, konsumsi daya berkurang, keamanan terjamin menurut *trusted computing group Open Algorithms (OPAL)*. Terlihat jauh perbedaan SSD SATA biasa dengan SSD NVMe, jika SSD hanya sanggup melayani 1 perintah dengan 32 antrian dalam satu waktu, maka NVMe bisa melayani 64.000 perintah dengan 64.000 antrian dalam satu waktu, bahkan SSD NVMe mampu menerima beberapa perintah lebih dari satu inti prosesor dan bisa memprioritaskan permintaan. Tabel 1 membandingkan performa *protocol* AHCI pada SSD SATA dan *protocol* NVMe pada SSD NVMe.

Tabel 1 Perbandingan performa SSD SATA teknologi AHCI dan SSD NVMe

Parameter	AHCI	NVMe
Pembacaan register yang tidak ter-*cache*	4 per perintah 8000 *cycles*	0 per perintah
MSI-x dan interupsi steering	Tidak	Ya
Pararel dan *Multiple Threads*	Rekomendasi sinkronasi, terkunci	Tidak terkunci
Maksimum antrian	1 antrian 32 perintah per 1 antrian	64 antrian 64 perintah per 1 antrian

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode NIST, metode ini menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui langkah-langkah dan alur penelitian secara sistematis sehingga dapat dijadikan pedoman dalam penyelesaian masalah yang ada dalam penelitian. Menurut Anggara (2017) melakukan teknik forensik dan analisis forensik berdasarkan metode yang benar akan memeliki keberhasilan hampir 100% dalam mengumpulkan data forensik. Tahapan NIST yaitu *collection*, *examination*, *analysis*, dan *reporting* yang ditunjukkan pada Gambar 4.

Gambar 4 Tahapan dalam metode NIST

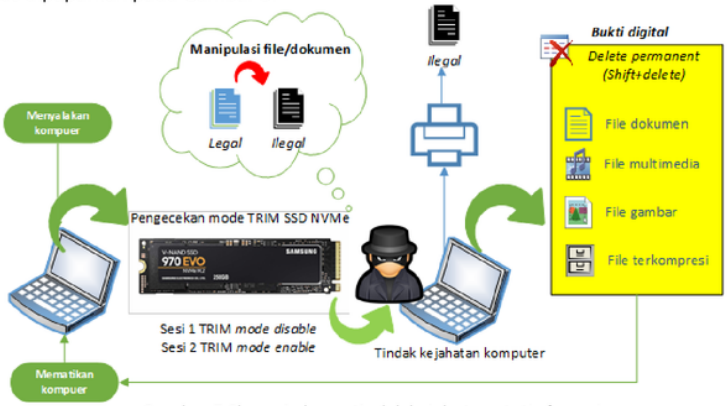
Penjelasan tahapan dan langkah-langkah dalam metode NIST adalah sebagai berikut:

a. *Collection*: Melakukan identifikasi, labeling, *record*, dan *retrieve* data dari sumber data yang relevan.
b. *Examination*: Melakukan pengolahan data yang dikumpulkan secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa bukti digital sesuai dengan yang didapat pada tempat kejadian kejahatan komputer, bukti digital perlu dilakukan validasi *file* yang ada pada bukti digital dengan *hasing*.
c. *Analysis*: Menganalisis pemeriksaan barang bukti secara teknis dan legal untuk mendapatkan informasi yang berguna untuk barang bukti digital serta dapat dipertanggungjawabkan secara ilmiah dan secara hukum.
d. *Reporting:* Pelaporan dilakukan setelah diperoleh barang bukti digital dari proses pemeriksaan data analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai tool, penjelasan metode yang digunakan dan memberikan rekomendasi untuk memperbaiki kebijakan, prosedur, peralatan dan aspek lain dari proses forensik.

Objek penelitan menggunakan SSD NVMe, *file* yang dijadikan barang bukti digital dibagi menjadi 4 kategori yaitu file dokumen, file multimedia, file gambar dan file kompresi. Alat dan bahan untuk mendukung proses investigasi forensik berupa perangkat keras dan perangkat lunak, perangkat keras yang diperlukan 1 pcs notebook yang sudah support SSD NVMe (komputer simulasi), 1 pcs notebook thinkpad yoga 14 corei7 ram 8gb (komputer akuisisi), 1 pcs SSD NVMe samsung 960 evo, 1 pcs *converter SSD NVMe to USB.* Perangkat lunak yang diperlukan Sistem operasi Windows 10 64bit, FTK Imager (Perangkat lunak akuisisi), Autopsy (perangkat lunak eksaminasi), Write Blocker (Perangkat lunak *read only storage*).

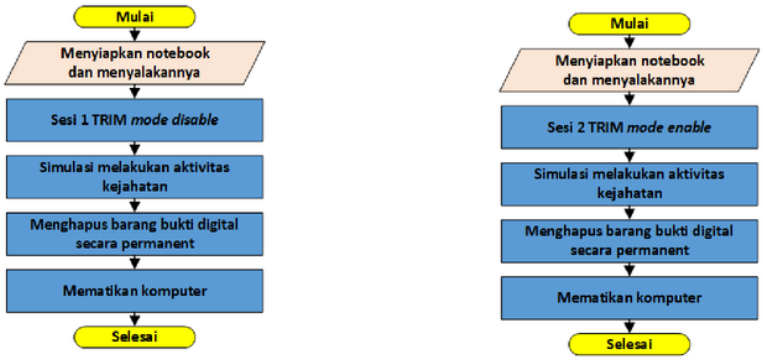
Skenario Kasus

Barang bukti dari hasil tindak kejahatan dijadikan sebagai obyek penelitian disimulasikan melalui skenario berikut: Menyiapkan notebook yang sudah *support* SSD NVMe dan menyalakannya, melakukan pengecekan dan mengaktifkan mode TRIM sesuai sesinya, melakukan aktivitas komputer sebagai tindak kejahatan, menghapus barang bukti kejahatan secara *permanent* dan mematikan komputer sesuai prosedur. Tahapan skenario kasus dipaparkan pada Gambar 5.



Gambar 5 Skenario kasus tindak kejahatan *static forensics*

Rancangan skenario implementasi dibagi menjadi 2 sesi, sesi yang pertama TRIM *mode disable* dan sesi kedua dengan TRIM *mode enable*. Tahapan skenario dipaparkan pada Gambar 6.



Gambar 6 *flowchart* proses skenario

Sesi pertama menonaktifkan fitur TRIM pada SSD NVMe melalui *command line* pada sistem operasi Windows dengan perintah "fsutil behavior set disabledeletenotify 1", simulasi melakukan aktivitas tindak kejahatan memanipulasi *file* dan menghapus barang bukti digital secara *permanent (shift+delete)* dan mematikan komputer sesuai prosedur. Sesi kedua mengaktifkan fitur TRIM melalui *command line* dengan perintah "fsutil behavior set disabledeletenotify 0", simulasi melakukan tindak kejahatan pada komputer dengan memanipulasi *file* ilegal dan menghapus barang bukti secara *permanent (shift+delete)* dan mematikan komputer sesuai prosedur.

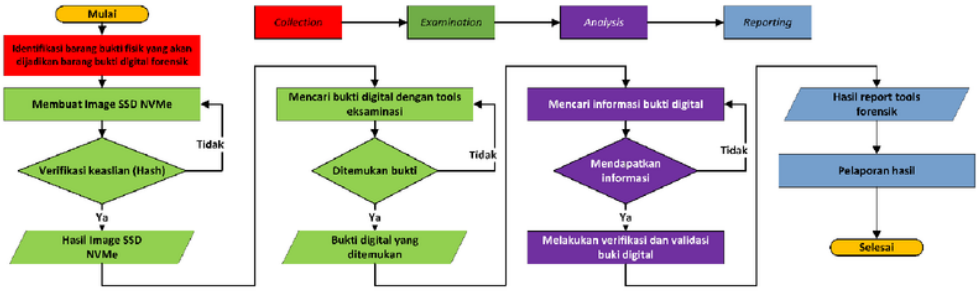
4. HASIL DAN PEMBAHASAN

Tahapan implementasi dan pengujian dilakukan sesuai dengan desain skenario yang dibuat, tahapan pertama yaitu *Collection*, setelah menerima sebuah kasus kejahatan komputer investigator mengidentifikasi barang bukti fisik yang layak dan relevan untuk diajukan sebagai barang bukti digital.

Tahapan kedua yaitu *Examination*, proses ini dibagi menjadi dua proses yaitu proses akuisisi dan proses analisis. Proses pertama akuisisi yaitu membuat image SSD NVMe dengan menggunakan aplikasi FTK Imager dibantu dengan aplikasi *write blocker* untuk menjaga keaslian dan tidak ada perubahan data digital pada saat akuisisi. Setelah image bukti digital dibuat dilakukan pengecekan nilai *hashing*. Proses kedua yaitu eksaminasi menggunakan perangkat lunak *forensics* yang telah disiapkan untuk menemukan bukti digital.

Tahapan ketiga yaitu *Analysis*, barang bukti digital yang didapat dianalisis terhadap jenis file, kapan file tersebut dibuat dan mencari nilai *hash* pada bukti digital tersebut. Kemudian dilakukan verifikasi dan validasi bukti digital. Pada proses ini perlu kehati-hatian, jika salah memberikan informasi terkait barang bukti maka kesimpulan peradilan juga akan salah.

Tahapan terakhir yaitu *Reporting*, proses ini memberikan informasi terkait bukti digital yang ditemukan, bukti digital pada kasus atau penelitian ini menerapkan verifikasi dan validasi berdasarkan nilai *hash*. Hasilnya dibandingkan dengan beberapa tool yang sudah disiapkan terkait akurasi didapatkannya barang bukti, Gambar 7 *flowchart* yang digunakan untuk implementasi metode NIST.



Gambar 7 *flowchart* eksperimen menggunakan metode NIST

Hasil yang diharapkan pada penelitian ini adalah proses analisis berjalan dengan baik dan ditemukannya bukti digital dari SSD NVMe yang digunakan sebagai objek penelitian.

5. KESIMPULAN

Berdasarkan hasil eksperimen yang dilakukan, pengambilan bukti digital pada SSD NVMe dengan menggunakan metode NIST pada sistem operasi Windows dengan adanya fitur TRIM terbukti berpengaruh pada eksaminasi dan analisis *digital forensics*. Percobaan pertama SSD NVMe dengan fitur TRIM *mode disable*, sebagian besar data yang dihapus dapat di*recovery* kembali seperti halnya melakukan *recovery* data pada HDD. Percobaan kedua dengan *mode enable* pada TRIM hasil yang didapatkan sebagian data yang terhapus tidak dapat *direcovery* kembali dengan kedua *tools* forensik. Dapat disimpulkan, bahwa fitur TRIM yang ada pada sistem operasi Windows dan SSD NVMe dapat menjadi hambatan dalam analisis dan eksaminasi *digital forensics*.

HASIL CEK_1808048032

ORIGINALITY REPORT

16%	15%	0%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	6%
2	publikasiilmiah.unwahas.ac.id Internet Source	3%
3	beon.co.id Internet Source	2%
4	endangkurniawan.com Internet Source	2%
5	publikasi.dinus.ac.id Internet Source	1%
6	Submitted to Universitas Islam Indonesia Student Paper	1%
7	arayamedia.id Internet Source	<1%
8	es.scribd.com Internet Source	<1%
9	f1000research.com Internet Source	<1%

10	id.123dok.com Internet Source	<1%
11	de.scribd.com Internet Source	<1%
12	Submitted to Udayana University Student Paper	<1%
13	hagaipantoro.blogspot.com Internet Source	<1%
14	docobook.com Internet Source	<1%
15	Submitted to Atma Jaya Catholic University of Indonesia Student Paper	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		